# DATA HIDING THROUGH ARRANGEMENT OF OBJECTS

## Related Application Data

**[0001]** The present application is a continuation in part of U.S. Patent Application No.
*now U.S. Pat. No. 6,345,104*
09/127,502, filed July 31, 1998 (allowed), which is a continuation-in-part of U.S. Patent
*now U.S. Pat No. 6,449,377*
Application No. 09/074,034, filed May 6, 1998. The 09/127,502 application is also a

continuation-in-part of U.S. Patent Application No. 08/967,693, filed November 12, 1997 (now

Patent 6,122,392), which is a continuation of application 08/614,521, filed March 15, 1996 (now

Patent 5,745,604), which is a continuation of application 08/215,289, filed March 17, 1994 (now

abandoned). The 09/127,502 application is also a continuation-in-part of application 08/649,419,

filed May 16, 1996 (now Patent No. 5,862,260). The 09/127,502 application also claims the

benefit of U.S. Provisional application 60/082,228, filed April 16, 1998. The present application

also claims the benefit of assignee's U.S. Provisional Patent Application No. 60/350,505, filed

January 18, 2002, titled "Data Hiding Through Arrangement of Objects."


**[0002]** The present application is also related to U.S. Patent Application No. 09/940,872, filed

August 27, 2001.


**[0003]** Each of the above-mentioned patent documents is herein incorporated by reference.


## Field of the Invention

**[0004]** The present invention relates to steganography and data hiding.


## Background and Summary of the Invention

**[0005]** Digital watermarking is a process for modifying physical or electronic media to embed a

machine-readable code into the media. The media may be modified such that the embedded code

is imperceptible or nearly imperceptible to the user, yet may be detected through an automated

detection process. Most commonly, digital watermarking is applied to media signals such as

images, audio signals, and video signals. However, it may also be applied to other types of

media objects, including documents (e.g., through line, word or character shifting), software,

multi-dimensional graphics models, and surface textures of objects.

5

[0006]   Digital watermarking systems typically have two primary components: an encoder that

embeds the watermark in a host media signal, and a decoder that detects and reads the embedded

watermark from a signal suspected of containing a watermark (a suspect signal). The encoder

embeds a watermark by altering the host media signal. The reading component analyzes a

10   suspect signal to detect whether a watermark is present. In applications where the watermark

encodes information, the reader extracts this information from the detected watermark.

[0007]   Several particular watermarking techniques have been developed. The reader is

presumed to be familiar with the literature in this field. Particular techniques for embedding and

15   detecting imperceptible watermarks in media signals are detailed in the assignee's co-pending

U.S. Patent Application No. 09/503,881 and U.S. Patent Application No. 6,122,403, which are

each herein incorporated by reference.

[0008]    In parent application no. 09/127,502 we disclose the following:

20   *Many security documents are still designed largely by hand.  A designer works at a drafting*

*table or computer workstation, and spends many hours laying-out minute (e.g. 5 mm x 5 mm)*

*excerpts of the design.  To aid integration of watermark and/or calibration pattern data in this*

*process, an accessory layout grid can be provided, identifying the watermark "bias" (e.g. -3 to*

*+3) that is to be included in each 250 micron cell of the security document.  If the accessory grid*

25   *indicates that the luminance should be slightly increased in a cell (e.g. 1%), the designer can*

*take this bias in mind when defining the composition of the cell and include a touch less ink than*

*might otherwise be included.  Similarly, if the accessory grid indicates that the luminance should*

*be somewhat strongly increased in a cell (e.g. 5%), the designer can again bear this in mind and*

2

*try to include more ink than might otherwise be included.  Due to the substantial redundancy of most watermark encoding techniques, strict compliance by the designer to these guidelines is not required.  Even loose compliance can result in artwork that requires little, if any, further modification to reliably convey watermark and/or calibration information.*

5

**[0009]**  *Such "designing-in" of embedded information in security documents is facilitated by the number of arbitrary design choices made by security document designers.  A few examples from U.S. banknotes include the curls in the presidents' hair, the drape of clothing, the clouds in the skies, the shrubbery in the landscaping, the bricks in the pyramid, the fill patterns in the*

10  *lettering, and the great number of arbitrary guilloche patterns and other fanciful designs, etc. All include curves, folds, wrinkles, shadow effects, etc., about which the designer has wide discretion in selecting local luminance, etc.  Instead of making such choices arbitrarily, the designer can make these choices deliberately so as to serve an informational -- as well as an aesthetic -- function.*

15

**[0010]**  *To further aid the security document designer, data defining several different information-carrying patterns (both watermark and/or calibration pattern) can be stored on mass storage of a computer a workstation and serve as a library of design elements for future designs.  The same user-interface techniques that are employed to pick colors in image-editing*

20  *software (e.g. Adobe Photoshop) and fill textures in presentation programs (e.g. Microsoft PowerPoint) can similarly be used to present a palette of information patterns to a security document designer.  Clicking on a visual representation of the desired pattern makes the pattern available for inclusion in a security document being designed (e.g. filling a desired area).*

25  **[0011]**  *In the embodiment earlier-described, the calibration pattern is printed as a visible artistic element of the security document.  However, the same calibration effect can be provided subliminally if desired.  That is, instead of generating artwork mimicking the gray-scale pattern of the reference calibration block, the reference calibration block can itself be encoded into the*

3

*security document as small changes in local luminance. In many such embodiments, the bias to localized document luminance due to the calibration pattern is simply added to the bias due to the watermark data, and encoded like the watermark data (e.g. as localized changes to the width or position of component line-art lines, as inserted ink droplets, etc.).*

5

[0012]   The present invention continues these inventive ideas. According to one aspect of the present invention, message objects are included in an image. The message objects preferably have characteristics that distinguish them from image background or other image objects. Some such distinguishing characteristics many include, color or gray-scale values, luminance values, and a contrast in comparison to other objects or to a background. The distinguishing characteristics can be subtle and need not be perceptible by a human viewer. For example, the message object may be slightly lighter than the image background or other image objects. Or the message objects may be darker than its background.

[0013]   Message objects are arranged within the image to convey (or hide) information, such as a steganographic message or signal. The message is typically indistinguishable by a human viewer. However, computer software can analyze the arrangement to determine the hidden information. In one embodiment, a digital watermark signal is reduced to a set of spatial positions. The set of spatial positions sufficiently conveys the digital watermark signal. Message objects are positioned according to the set of spatial points. Non-message objects are combined with the message objects to form an image or design. The message objects include distinguishable characteristics, e.g., via color, contrast, gray-scale level or luminance, in comparison to the non-message objects. The digital watermark signal is detected by distinguishing the message objects from the non-message objects (e.g., via color or contrast differences) and analyzing the relative placement of the message objects within the image or design.

**[0014]**  Additional features and advantages of the present invention will become even more apparent with reference to the following detailed description and accompanying drawings.

## Brief Description of the Drawings

**[0015]**  Fig. 1 is a flow diagram illustrating an image construction method according to one aspect of the present invention.

**[0016]**  Fig. 2 illustrates a digital watermark signal.

**[0017]**  Fig. 3 illustrates a representation of the Fig. 2 watermark signal after thresholding.

**[0018]**  Fig. 4 illustrates a gray-scale image including message objects.

## Detailed Description

**[0019]**  We have found that the arrangement of objects within an image can be used to convey information – which is otherwise imperceptible to a human viewer.  We arrange so-called "message objects" to convey or represent a steganographic signal (e.g., a digital watermark).  We define a message object broadly herein as including an information carrier, an image object, a shape, an object or collection of objects, a pixel or group of pixels, a contrast or color/gray-scale area, etc.  A set of message objects is arranged within an image or area to form a steganographic message.  A few examples are provided below.

**[0020]**  Consider a drawing illustrating a Dalmatian puppy.  The puppy has a white coat complimented with black spots.  An artist (or digital editor) can arrange the spots -- an example of a message object -- so as to convey a hidden or steganographic message.  More practical,

however, is to align the spots according to a predetermined steganographic signal and then sculpt or design the puppy around the aligned spots.

[0021]   Now consider an image or picture depicting hundreds of marbles strewn across a
5     surface.  Certain of the marbles have an offsetting color (or luminance, gray-scale level, contrast, etc.) when compared to the surface or to other marbles.  We call these offset color marbles our "message marbles."  The message marbles are arranged to represent (or to form) a steganographic signal.  More practical, perhaps, is to initially arrange the message marbles according to a predetermined signal (e.g., a digital watermark signal, an orientation signal or
10   various combinations of both) and then "fill-in" non-message marbles to complete the image.

[0022]   Another example is particularly appealing to our astronomy friends.  Consider an image or graphic depicting a nighttime sky.  The sky is populated with "message stars."  The message stars are arranged in the nighttime sky in a predetermined manner according to a steganographic
15   signal.  The sky is further populated with non-message stars.  The message stars are preferably distinguishable from the non-message stars.  The distinguishing characteristics need not be visibly perceptible, and may be based on subtle differences, e.g., as measured in luminance, color levels, brightness, contrast, etc.

20   [0023]   A steganographic decoder, analyzing a digital version (e.g., an optically captured image) of the Dalmatian puppy, marble image or populated nighttime sky, decodes the steganographic message.

[0024]   While the above signal-conveying techniques rely on the arrangement of message
25   objects in a spatial domain (e.g., in an image), message formation or detection can be based in either a spatial or transform (e.g., Fourier or frequency) domain.  For example, the arrangement of the message objects in the spatial domain may have significance in a frequency domain (e.g., may correspond to a pattern of peaks, etc.).  Message detection can be accordingly facilitated,

e.g., as discussed in Assignee's U.S. Patent Application Nos. 09/940,872 and 09/503,881, each of which is herein incorporated by reference. The incorporated by reference patent documents detail many techniques for signal hiding and message detection.

5    [0025]    (Applicant notes that since the Fourier transform is a linear operation, adjustments to pixels in a region may be made in the frequency or spatial domain. For example, a digital watermark embedder can adjust the frequency domain representation of the host signal according to the watermark definition to form a frequency domain representation of the watermarked signal region, and then take the inverse Fourier transform of the watermarked regions to produce the

10   watermarked signal in the spatial domain. Alternatively, the embedder can compute a difference signal to effect the desired changes to the region in the frequency domain, and then compute the inverse transform of the difference signal into the spatial domain, where corresponding pixels of the difference signal and host signal region are summed. Either way, the result is a watermarked signal in the original domain of the host signal.).

15   Steganographic Image Construction

[0026]    We now describe our preferred image construction with reference to Figs. 1-4. Fig. 1 illustrates a flow diagram depicting method steps for a first embodiment of the present invention.

20   A digital watermark signal is provided in step 10. The watermark signal preferably includes a message component, e.g., a payload or identifier, and/or an orientation signal. An orientation signal is helpful to resolve image distortion such as scale and rotation. Fig. 2 illustrates an example of a watermark signal shown in a spatial domain. (We note that the Fig. 2 representation is exaggerated to help simplify the discussion.). Although not required, the digital

25   watermark signal is preferably a pure (or "raw") signal in that it does not include image data.

[0027]    Thresholding is applied to the Fig. 2 watermark signal (step 12). Thresholding preferable identifies (or reduces the watermark signal to) a set of relevant points. The relevant

7

points may correspond to or represent a wide range of features, such as signal or frequency peak

levels, magnitude peaks, watermark message components, watermark orientation references,

spatial domain signal characteristics, etc. Regardless of the relevant features used to determine a

relevant point, the set of relevant points is preferably sufficient to represent (or convey) the

5    watermark signal. (We use the term "thresholding" generally herein to include a process to

identify a set and location of spatial points for placement of message objects. Alternatively, the

thresholding may identify relevant frequency domain points, which can be mapped or ·

transformed into a spatial domain representation.) The thresholding procedure can also be

adjusted to provide a more or less robust watermark signal. For example, the spacing of relevant

10   points can be increased, but at a cost of robustness.

[0028]    While the term "thresholding" is used as an illustrative technique, the present invention

is not so limited. Indeed there are other ways to refine a watermark signal into a set or map of

relevant points. For example, a frequency analysis can be used to identify significant frequency

15   characteristics (e.g., peaks). These characteristics can be mapped to the spatial domain to

identify a placement point (e.g., a spatial location). Or, as in another implementation, the digital

watermark signal is quantitized, e.g., via a root mean square measurement. Of course other

techniques can be used to reduce a watermark signal to a set of relevant spatial points sufficient

to convey the signal.

20

[0029]    The set of relevant points comprises a placement map as shown in Fig. 3. (It should be

appreciated that there are many, many possible placement map patterns, including many more or

less significant positions. Fig. 3 illustrates but one such possible placement map.). The Fig. 3

placement map includes a plurality of spatial positions or points (e.g., 20 and 21). These points

25   guide the placement of message objects.

[0030]    In one alternative implementation, the placement map includes a relative contrast

indicator. For example, a placement map point may include a relatively darker or larger point

8

(20), indicating a need for a stronger contrast level (or color, gray-scale, etc.) of a message object, in comparison to a relatively lighter or smaller point (21). A higher contrast may signify a predetermined frequency domain characteristic, such as peak magnitude or frequency response, etc.

5

[0031]    Returning to Fig. 1, message objects are arranged according to the placement mapping (step 14). For example, message marbles (or message stars, black Dalmatian spots, etc.) are placed on or over (or otherwise placed corresponding to) the placement map points. The message objects thus convey the steganographic signal. Other image objects can be placed in the image, e.g., to fill in or otherwise populate the image.

10

Alternative Steganographic Images

[0032]    There are many alternative ways to implement our inventive steganographic techniques. Consider the following illustrative examples.

15

[0033]    Off-the-shelf digital image editing tools (e.g., as provided by Adobe) can be used to place message objects in an image. The operator selects a message object, adjusts the object contrast (or color/gray-level, etc.) to sufficiently set the object apart from other image objects or the image background, and then places the objects according to a digital watermark placement map. Of course this placement process can be automated.

20

[0034]    A farmer's field can be plowed or crops can be planted or cut to represent message objects, all arranged according to a steganographic placement map. An aerial image of the farmer's field then includes the steganographic message.

25

9

**[0035]** Different color tulips (or other flowers) can be planted according to a placement map. For example, groups of white tulips (e.g., message tulips) can be planted in an otherwise purple tulip field. An aerial image captures the field -- including the steganographic message.

5   **[0036]** Captured images can be used in advertisements, e.g., when the steganographic message carries a link (e.g., a URL or an identifier used to obtain a link). Assignee's U.S. Patent Application No. 09/571,422, filed May 15, 2000, discloses many suitable linking techniques that are expressly contemplated as being combined with the present invention. This patent application is herein incorporated by reference.

10

**[0037]** Our techniques can even be advantageously employed in the photo-mosaic field. (Photo-mosaic processes are even further discussed, e.g., in U.S. Patent Nos. 6,137,498 and 5,649,032, which are each incorporated herein by reference.). As disclosed in U.S. Patent No. 6,137,498, a mosaic image is formed from a database (or collection) of source images. Source images are analyzed, selected and organized to produce the mosaic image. A target image is divided into tile regions, each of which is compared with individual source image portions to determine the best available matching source image. Positioning respective best-matching source images at the respective tile regions forms the mosaic image.

15

**[0038]** An improvement to a photo-mosaic process is to arrange message source photos (e.g.,
20   representing message objects) according to a watermark placement map. Preferably, the message source photos are subtly distinguishable from other mosaic photos via a gray-scale value, a color value, contrast or luminance, etc. The message source photos form (or convey) a steganographic signal. In one implementation, the arrangement of message source photos is carried out via the "best available matching" discussed above with respect to the 6,137,498 patent. In a first
25   implementation, the process determines whether a selected best available photo is to be titled over a placement map position. If so, the photo characteristics (luminance, contrast, gray-scale, etc.) are subtly altered to create a message source photo. In a second implementation, the "best

available matching" algorithm includes selection criteria, e.g., if selecting a photo for a placement map position, the algorithm selects a photo with sufficient distinguishing characteristics to qualify as a message object. The distinguishing characteristics can be measured in terms of its neighbors (e.g., a message photograph may include an overall different contrast,

5      color or gray-scale level from its neighboring photographs) or in terms of non-message photographs. In a third implementation, message source photos are arranged according to a placement map, and then other source photos are used to fill in or complete the photo mosaic. In a variation of this third implementation, the other, non-message source photos are selected and

10     arranged according to a best available matching technique.

[0039]    Similar embedded designs can be made using coins, bills, umbrellas, coffee mugs, opened or closed blinds in an apartment building, shapes, snow flakes, groups of pixels, etc., etc.

[0040]    With reference to Fig. 4, message objects of different colors (or gray-levels, tones, contrasts, luminance, etc.) can be used in the same image. For example, the Fig. 4 image

15     includes a gray background (shown by the diagonal hashes). A message object can be distinguished from the background if it is either lighter 30 or darker 31 than the background. Or if the background is blue, message objects can be red or green, etc.

20     <u>Message Detection</u>

[0041]    An image created according to our inventive techniques can be read using steganographic or digital watermarking decoding techniques, e.g., as described in assignee's 09/571,422 and/or 09/503,881 applications. In one implementation, Digimarc MediaBridge

25     watermark reading software, available from Digimarc Corporation headquartered in Tualatin, OR, is used to read an image including a corresponding MediaBridge digital watermark signal represented through our message object arranging techniques. Of course, other decoding

11

techniques can be used, particularly when they correspond to the techniques used to generate the original watermark signal. (For example, when using a Digimarc MediaBridge reader, the watermark signal is preferably created using a MediaBridge signal generator or embedder.). Most commonly, the reader identifies the message objects from the different levels of contrast (or

5      color, gray-scale, luminance, etc.) between a message object and other objects or background.


Conclusion


[0042]   The foregoing are just exemplary implementations of the present invention. It will be

10     recognized that there are a great number of variations on these basic themes. The foregoing illustrates but a few applications of the detailed technology. There are many others.


[0043]   To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference, in their entireties, the disclosures of the above-cited patents

15     and applications. The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this application and the incorporated-by-reference patents/applications are expressly contemplated.


20     [0044]   One application uses our inventive embedding techniques for "long-distance" or aerial digital watermark reading, e.g., for some of the traffic monitoring examples disclosed in Assignee's U.S. Provisional Patent Application No. 60/327,687, filed October 5, 2001. (In one experiment we created a digitally watermarked image using our inventive object placement techniques disclosed herein. We then optically captured an image of the watermarked image

25     with a digital camera augmented with a telescope. The watermarked image was about 100 feet away from the camera/telescope. The watermark was successfully detected.).

**[0045]** Although not belabored herein, artisans will understand that the systems and methods described above can be implemented using a variety of hardware and software systems. Alternatively, dedicated hardware, or programmable logic circuits, can be employed for such operations.

5

**[0046]** The various section headings in this application are provided for the reader's convenience and provide no substantive limitations. The features found in one section may be readily combined with those features in another section.

10

**[0047]** In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.